IN THE CLAIMS

Please amend the claims to read as follows:

1.   (Previously Presented)   A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

     a.   a user registration step, wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;

     b.   formation of a user-customizable rule module customized to the user in a rule module clearinghouse, wherein at least one pattern data of a user is associated with at least one execution command of the user;

     c.   a user identification step, wherein the electronic identicator compares a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user;

     d.   a command execution step, wherein upon successful identification of the user at least one previously designated rule module of the user is invoked to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the user presenting smartcards or magnetic swipe cards.

2.   (Original)   The method of claim 1 wherein during the command execution step, the electronic rule module clearinghouse communicates with one or more third-party computers.

3.   (Previously Presented)   The method of claim 1 wherein said execution commands are comprised of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules.

4.   (Previously Presented)   The method of claim 1 wherein pattern data comprises one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing

patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature.

5.   (Previously Presented)   The method of claim 1, wherein pattern data for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

6.   (Previously Presented)   The method of claim 1, wherein an execution command for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

7.   (Original)   The method of claim 1 further comprising a user re-registration check step, wherein the user's registration biometric sample is compared against previously registered biometric samples wherein if a match occurs, the computer system is alerted to the fact that the user has attempted to re-register with the electronic identicator.

8.   (Previously Presented)   The method of claim 1 wherein the biometric sample comprises one or more of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print.

9.   (Original)   The method of claim 1 wherein during the identification step, the user provides a personal identification code to the electronic identicator along with a bid biometric sample for purposes of identifying the user.

10.   (Original)   The method of claim 9 further comprising a biometric theft resolution step, wherein a user's personal identification code is changed when the user's biometric sample is determined to have been fraudulently duplicated.

11.   (Original)   The method of claim 1, wherein execution of an execution command authorizes the user to access stored electronic data.

Docket No. 8514-025   Page 3 of 34   Application No. 09/398,914

PAGE 6/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

12. (Original)   The method of claim 11 wherein accessing stored electronic data results in activation of an Internet-connected device.

13. (Original)   The method of claim 1 wherein executing an execution command processes electronic data to provide the user with a user requested electronic transmission.

14. (Previously Presented)   The method of claim 13, wherein said processing comprises invoking one or more of the following: a user's digital certificate, a user's identity scrambler, a user's interactive electronic consumer loyalty or consumer rewards program, a user's interactive electronic advertising, a user's interactive instant messaging program, a user's email authentication, and an automated electronic intelligent agent for electronic data search and retrieval that is customized to the user's requests.

15. (Original)   The method of claim 1 wherein executing an execution command presents electronic data that is customized to the user's requested electronic transmission.

16. (Original)   The method of claim 1 further comprising a user log-in repeat step, wherein during an electronic transmission the user is periodically required by the electronic identicator to present the user's bid biometric sample or at least one of the user's pattern data.

17. (Previously Presented)   The method of claim 1 further comprising a communications step wherein one or more of the following is used: the Internet, an intranet, an extranet, a local area network, and a wide area network.

18. (Previously Presented)   The method of claim 1 further comprising a third-party registration step, wherein a third-party registers identification data with the electronic identicator, the identification data comprising one or more of the following: a biometric, a digital certificate, an Internet protocol address, and a biometric input apparatus hardware identification code.

19.   (Original)   The method of claim 18 further comprising a third-party identification step, wherein a third-party providing the user with electronic transmissions is identified by the electronic identicator by comparing the third-party's bid identification data with the third-party's registered identification data.

20.   (Previously Presented)   A computer system device for tokenless biometric processing of electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, comprising:

  a.   a biometric input apparatus, for providing a bid or registration biometric sample of a user to the electronic identicator, wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;

  b.   an electronic rule module clearinghouse, having at least one user-customizable rule module further comprising at least one pattern data of the user associated with at least one execution command of the user, for executing at least one electronic transmission;

  c.   an electronic identicator, for comparing the bid biometric sample with registered biometric samples of users;

  d.   a command execution module, for invoking at least one previously designated execution command in the electronic rule module clearinghouse to execute an electronic transmission;

  wherein no smartcards or magnetic swipe cards are presented by the user to conduct the electronic transmission.

21.   (Original)   The device of claim 20 wherein the command execution module communicates with one or more third-party computers.

22.   (Previously Presented)   The device of claim 20 wherein pattern data comprises one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant

Docket No. 8514-025   Page 5 of 34   Application No. 09/398,914

PAGE 8/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

messaging address, personal medical records, an electronic audio signature, and an electronic visual signature.

23.   (Previously Presented)   The device of claim 20, wherein pattern data for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

24.   (Previously Presented)   The device of claim 20, wherein an execution command for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

25.   (Previously Presented)   A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

   a.   a primary and subordinated user registration step, wherein a primary and subordinated user each register with an electronic identicator at least one registration biometric sample taken directly from the person of the primary and subordinated user, respectively;

   b.   formation of a rule module customized to the primary and subordinated user in a rule module clearinghouse, wherein at least one pattern data of the primary and subordinated user is associated with at least one execution command of the primary and subordinated user, the rule module customized to the primary user is customizable by the primary user and the rule module customized to the subordinated user is customizable by the subordinated user;

   c.   a subordinated user identification step, wherein the electronic identicator compares a bid biometric sample taken directly from the person of the subordinated user with at least one previously registered biometric sample for producing either a successful or failed identification of the subordinated user;

   d.   a subordination step wherein upon successful identification of the subordinated user, the pattern data of the subordinated user is searched to determine if any of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules; and

   e.   a command execution step, wherein upon the successful identification of the subordinated user and the determination that at least one of the subordinated user's rule

Docket No. 8514-025   Page 6 of 34   Application No. 09/398,914

modules is subordinated to at least one of the primary user's rule modules, at least one previously designated execution command of the primary user is invoked to execute at least one electronic transmission;

        wherein a biometrically authorized electronic transmission is conducted without the primary and subordinated user presenting smartcards or magnetic swipe cards.

        26.   (Previously Presented)   The method of claim 3 wherein execution commands for accessing stored electronic data include permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

        27.   (Previously Presented)   The method of claim 26 wherein accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital.

        28.   (Previously Presented)   The method of claim 26 wherein accessing membership benefits further comprises one or more of the following: validating a user's eligibility to rent videos under their pre-paid membership; validating a user's eligibility to access an Internet web site; and validating a user's eligibility to enter a real-time internet chat room with other people on-line.

        29.   (Previously Presented)   The method of claim 26 wherein accessing event admittance further comprises one or more of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-rated film being shown in theatres; and validating a user's eligibility to board a vehicle of travel.

        30.   (Previously Presented)   The method of claim 11 wherein accessing stored electronic data comprises accessing one or more of the following: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content;

Docket No. 8514-025   Page 7 of 34   Application No. 09/398,914

PAGE 10/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

on-line messaging content; on-line educational content; on-line academic examination-taking;

on-line personalized medical and health content; and server-based computer software

programs and hardware drivers.

31.   (Previously Presented)   The method of claim 1 wherein at least one rule

module further comprises one or more of the following: at least one pattern data associated

with at least two execution commands; and at least one execution command associated with

at least two pattern data.

32.   (Previously Presented)   The method of claim 12 wherein activation of an

internet-connected device further comprises activating one or more of the following devices:

a wireless pager; a wireless telephone; a network computer; an exercise machine; a television;

an electronic book; a radio; a household appliance; a personal digital assistant; a photocopy

machine; and a digital audio player.

33.   (Previously Presented)   The method of claim 14 wherein the automated

intelligent agent for electronic data search and retrieval further comprises conducting

periodic, user-customized on-line retrievals for one or more of the following data: medical

updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice

over internet phone calls; electronic advertisements; and faxes.

34.   (Previously Presented)   The method of claim 29 wherein the vehicle of

travel further comprises one or more of the following: an airplane; a train; a boat; and a bus.

35.   (Previously Presented)   The method of claim 14 wherein the automated

intelligent agent can extrapolate from the user's existing preferences and on-line activity

patterns to automatically and periodically recommend to the user new data that may expand

and delete the user's pattern data and execution commands based upon the intelligent agent's

algorithmic projection of what the user's on-line preferences and activities will be in the

future.

36.   (Previously Presented)   The method of claim 14 wherein invoking a

user's digital certificate with an electronic transmission to verify the authenticity of the

sender and the electronic document's contents to yield a secure, authenticated electronic transmission.

37.   (Previously Presented)   The method of claim 13 wherein the processing of electronic transmissions further comprises execution commands which filter the access and presentation of data when the user is subordinated user.

38.   (Previously Presented)   The method of claim 37 wherein the filter governs subordinated user access to one or more of the following: Internet web sites with adult content; Internet sites with violent content; on-line session length; and educational on-line resources which are automatically "pushed" to the subordinated user during a particular on-line session, as pre-determined by the primary user.

39.   (Previously Presented)   The device of claim 20 wherein execution commands for accessing stored electronic data include permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

40.   (Previously Presented)   The device of claim 39 wherein accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital.

41.   (Previously Presented)   The device of claim 39 wherein accessing membership benefits further comprises one or more of the following: validating a user's eligibility to rent videos under their pre-paid membership; validating a user's eligibility to access an Internet web site; and validating a user's eligibility to enter a real-time internet chat room with other people on-line.

42.   (Previously Presented)   The device of claim 39 wherein accessing event admittance further comprises one or more of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-

rated film being shown in theatres; and validating a user's eligibility to board a vehicle of travel.

43.   (Previously Presented)   The device of claim 20 wherein execution commands further comprise accessing one or more of the following stored electronic data: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content; on-line messaging content; on-line educational content; on-line academic examination-taking; on-line personalized medical and health content; and server-based computer software programs and hardware drivers.

44.   (Previously Presented)   The device of claim 20 wherein at least one rule module further comprises one or more of the following: at least one pattern data associated with at least two execution commands, and at least one execution command associated with at least two pattern data.

45.   (Previously Presented)   The device of claim 20 wherein execution commands further comprise activation of one or more of the following Internet-connected devices: a wireless pager; a wireless telephone; a network computer; an exercise machine; a television; an electronic book; a radio; a household appliance; a personal digital assistant; a photocopy machine; and a digital audio player.

46.   (Previously Presented)   The device of claim 20 wherein execution commands further comprise an automated intelligent agent for electronic data search and retrieval which conducts periodic, user-customized on-line retrievals for one or more of the following data: medical updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice over internet phone calls; electronic advertisements; and faxes.

47.   (Previously Presented)   The device of claim 42 wherein the vehicle of travel further comprises one or more of the following: an airplane; a train; a boat; and a bus.

48.   (Previously Presented)   The device of claim 46 wherein the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand

and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future.

49.   (Previously Presented)   The device of claim 20 wherein execution commands further comprise invoking a user's digital certificate with an electronic transmission to verify the authenticity of the sender and the electronic document's contents to yield a secure, authenticated electronic transmission.

50.   (Previously Presented)   The device of claim 20 wherein execution commands further comprise the processing of electronic transmissions which filter the access and presentation of data when the user is subordinated user.

51.   (Previously Presented)   The device of claim 50 wherein the filter governs subordinated user access to one or more of the following: Internet web sites with adult content; Internet sites with violent content; on-line session length; educational on-line resources which are automatically "pushed" to the subordinated user during a particular on-line session, as pre-determined by the primary user.

52.   (Previously Presented)   The method of claim 4 wherein said execution commands are comprised of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules.

53.   (Previously Presented)   The method of claim 53 wherein execution commands for accessing stored electronic data include permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

54.   (Previously Presented)   A biometric method implemented in a computer system for processing electronic transmissions, comprising:

Docket No. 8514-025   Page 11 of 34   Application No. 09/398,914

registering at least one registration biometric sample taken directly from a user;

forming a user-customizable rule module customized to the user in a rule module clearinghouse, the rule module associating at least one pattern data of the user with at least one execution command of the user;

comparing a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed match; and

invoking the rule module of the user upon a successful match to execute at least one electronic transmission.

55.   (Previously Presented)   The method of claim 54, wherein the electronic transmission is executed without the user presenting smartcards or magnetic swipe cards.

56.   (Previously Presented)   The method of claim 54, wherein registering at least one registration biometric sample includes:

registering a plurality of biometric samples from a plurality of users; and

basketing a subset of the plurality of samples to facilitate the comparison with the bid biometric sample.

57.   (Previously Presented)   The method of claim 54, wherein comparing a bid biometric sample includes comparing the bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user.

58.   (Previously Presented)   The method of claim 54, wherein:

the execution command includes of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules; and

the execution command for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

59.   (Previously Presented)   The method of claim 54, wherein the execution command includes permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

60.   (Previously Presented)   The method of claim 59, wherein:
        the pattern data includes one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature; and
        the pattern data for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

61.   (Previously Presented)   The method of claim 54, wherein:
        the pattern data includes one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature; and
        the pattern data for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

62.   (Previously Presented)   The method of claim 54, wherein:
        the pattern data includes demographic information of the user; and

the execution command includes accessing stored electronic data to determine eligibility to purchase restricted products or to access data or services.

63.   (Previously Presented)   A biometric method implemented in a computer system for processing electronic transmissions, comprising:

registering at least one primary registration biometric sample taken directly from a primary user;

registering at least one secondary registration biometric sample taken directly from a secondary user;

forming a primary user-customizable rule module customized to the primary user in a rule module clearinghouse, the primary rule module associating at least one primary pattern data of the primary user with at least one primary execution command of the primary user;

forming a secondary user-customizable rule module customized to the secondary user in the rule module clearinghouse, the secondary rule module associating at least one secondary pattern data of the user with at least one secondary execution command of the secondary user;

subordinating the secondary rule module to the primary rule module;

comparing a bid biometric sample taken directly from the person of the secondary user with at least one previously registered biometric sample for producing either a successful or failed match;

determining that the secondary rule module is subordinated to the primary rule module; and

invoking the primary rule module of the primary user upon a successful match to execute at least one electronic transmission.

64.   (Previously Presented)   A computer system device for biometric processing of electronic transmissions, comprising:

a biometric input apparatus, for providing a bid or registration biometric sample of a user;

an electronic rule module clearinghouse, having at least one user-customizable rule module including at least one pattern data of the user associated with at least one execution command of the user;

Docket No. 8514-025   Page 14 of 34   Application No. 09/398,914

PAGE 17/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

an electronic identicator, to compare at least one registration biometric sample stored in the electronic identicator with a bid biometric sample to produce either a successful or failed match; and

a command execution module, to invoke at least one execution command in the electronic rule module clearinghouse to execute an electronic transmission.

65.   (Previously Presented)   The computer system of claim 64, wherein the electronic transmission is executed without the user presenting smartcards or magnetic swipe cards.

66.   (Previously Presented)   The computer system of claim 64, further comprising:

storage for a plurality of registration biometric samples from a plurality of users; and

means for basketing a subset of the plurality of samples in the storage to facilitate the comparison with the bid biometric sample.

67.   (Previously Presented)   The computer system of claim 64, wherein the electronic identicator is operative to compare at least one registration biometric sample stored in the electronic identicator with the bid biometric sample to produce either a successful or failed identification of the user.

68.   (Previously Presented)   The computer system of claim 64, wherein:

the execution command includes of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules; and

the execution command for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

69.   (Previously Presented)   The computer system of claim 64, wherein:

the pattern data includes one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, a non-financial data repository account, a telephone number, a mailing address, purchasing

patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature; and

the pattern data for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

70.   (Previously Presented)   The computer system of claim 69, wherein the execution command for accessing stored electronic data includes permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

71.   (Previously Presented)   The computer system of claim 64, wherein the execution command for accessing stored electronic data includes permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

72.   (Previously Presented)   The computer system of claim 64, wherein:
the pattern data includes demographic information of the user; and
the execution command includes accessing stored electronic data to determine eligibility to purchase restricted products or to access data or services.

73.   (New) A method for providing approval of an age-restricted transaction conducted by an age presenter, comprising:
receiving, at an unattended age verification station, at least one biometric sample proffered by the age presenter via a biometric identification device;

Docket No. 8514-025   Page 16 of 34   Application No. 09/398,914

PAGE 19/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

sending the at least one biometric sample to at least one database, wherein the at least one database has at least one biometric record stored therein, wherein the at least one biometric record contains a reference of the age presenter's age;

comparing, at the at least one database, the at least one biometric sample to the at least one biometric record stored in the at least one database;

making a first determination, at the at least one database, whether the at least one biometric sample matches the at least one biometric record stored in the at least one database;

in the event the at least one biometric sample matches the at least one biometric record stored in the at least one database, making a second determination whether the age presenter's age information in the reference meets at least one system parameter;

in the event that the age mapped to the biometric record meets the at least one system parameter, approving the age-restricted transaction at the at least one database; and

receiving, at the unattended age verification station, confirmation of the age-restricted transaction approval.

74.   (New) The method of claim 73, wherein the at least one system parameter is defined by the age verification station.

75.   (New) The method of claim 73, wherein the at least one biometric sample comprises at least one of a fingerprint scan, an iris scan, a facial scan, a voice scan, a retinal scan, a hand architecture scan, a vein pattern scan, a signature sample, and a DNA sample.

76.   (New) The method of claim 73, wherein the at least one biometric record comprises at least one digital representation of a fingerprint scan, an iris scan, a facial scan, a voice scan, a retinal scan, a hand architecture scan, a vein pattern scan, a signature sample, and a DNA sample.

77.   (New) The method of claim 73, wherein the steps of sending and receiving comprise sending and receiving encrypted data.

78.   (New) The method of claim 73, wherein sending the at least one biometric sample to the at least one database further comprising sending at least one of a location for the unattended age verification station, a time of age-restricted transaction, a transaction type, a reference code, a detailed access record, and blood alcohol content of the age presenter.

Docket No. 8514-025   Page 17 of 34   Application No. 09/398,914

79.   (New) The method of claim 73, wherein a system user's information is stored in the at least one database.

80.   (New) The method of claim 79, wherein transaction information pertaining to the age-restricted transaction is compared to the system user information stored in the at least one database.

81.   (New) The method of claim 73, wherein the unattended age verification station is selected from the group consisting of a vending machine, a kiosk, a PC, a wireless device, a computing device, and a storage device.

82.   (New) The method of claim 73, wherein the unattended age verification station is an unattended point of sale device.

83.   (New) The method of claim 82, wherein the age-restricted transaction comprises a financial transaction.

84.   (New) The method of claim 83, wherein the financial transaction settlement is conducted via a financial transaction system, wherein the financial transaction system comprises the at least one biometric sample being used to authenticate the financial transaction settlement.

85.   (New) The method of claim 73, wherein the second determination comprises a reliability determination and includes assessing whether or not the at least one biometric sample is being used fraudulently.

86.   (New) A method for providing approval of an age-restricted transaction conducted by an age presenter, comprising:

receiving, at an unattended age verification station, at least one biometric sample proffered by the age presenter via a biometric identification device;

receiving, at the unattended age verification station, at least one identification code proffered by the age presenter;

Docket No. 8514-025   Page 18 of 34   Application No. 09/398,914

PAGE 21/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

sending the identification code proffered by the age presenter from the unattended age verification station to at least one database;

wherein the at least one database has at least one biometric record stored therein, wherein the at least one biometric record contains a reference of the age presenter's age, and wherein the at least one database has at least one identification code record;

comparing, at the at least one database, the at least one identification code to the at least one identification code record;

making, at the at least one database, a first determination whether the at least one identification code matches at least identification code record;

in the event the at least one identification code matches the at least one identification code record, making a second determination whether the reference meets at least one system parameter;

in the event the reference meets the at least one system parameter, pre-approving, at the at least one database, the at least one biometric record as a potential matching biometric record;

receiving, at the unattended age verification station, the potential matching biometric record from the at least one database;

comparing, at the unattended age verification station, the at least one biometric sample with the potential matching biometric record;

making, at the unattended age verification station, a third determination whether the at least one biometric sample matches the potential matching biometric record;

in the event that the at least one biometric sample matches the potential matching biometric record;

making, at the unattended age verification station, a fourth determination whether the matching biometric record was pre-approved at the at least one database; and

in the event the matching biometric record was pre-approved at the at least one database, approving, at the unattended age verification station, the age-restricted transaction.

87.   (New) The method of claim 86, further comprising the age verification station sending to the at least one database confirmation of completion of the age-restricted transaction.

88.   (New) The method of claim 86, wherein the at least one identification code comprises at least one of a unique number, a reasonably unique number, and a non unique number.

89.   (New) The method of claim 86, wherein a system user information is stored in the at least one database.

90.   (New) The method of claim 89, wherein a transaction information pertaining to the age-restricted transaction is compared to the system user information stored in the at least one database.

91.   (New) A method for providing approval of an age-restricted transaction conducted by an age presenter, comprising:

receiving, at an unattended age verification station, at least one biometric sample proffered by the age presenter via a biometric identification device;

receiving, at the unattended age verification station, at least one age-restricted action proposal proffered by the age presenter;

associating at least one proposal code with the at least one age-restricted action proposal;

sending an identification code proffered by the age presenter from the unattended age verification station to at least one database;

wherein the at least one database has at least one biometric record stored therein, wherein the at least one biometric record contains a reference of the age presenter's age, and wherein the at least one database has at least one identification code record;

sending the at least one proposal code affiliated with the age-restricted action proposal proffered by the age presenter from the unattended age verification station to the database;

comparing, at the at least one database, the at least one biometric sample to the at least one biometric record;

making a first determination, at the at least one database, whether the biometric sample matches the at least one biometric record;

in the event the at least one biometric sample matches the at least one biometric record, making a second determination whether the reference meets a parameter, wherein the parameter is indicated by the at least one proposal code;

in the event the reference meets the parameter, approving the age-restricted transaction at the at least one database; and

receiving, at the unattended age verification station, confirmation of the age-restricted transaction approval.

92.   (New) A method for enrolling a system user in a transaction system comprising:

providing at least one unattended age verification station, wherein the least one unattended age verification station is configured to access at least one database, wherein the at least one database has at least one biometric record stored therein, wherein the at least one biometric record is associated with the system user and contains a reference of the age presenter's age;

prompting the system user to proffer an enrollment data comprising age information, personal information, and at least one biometric samples;

transmitting to the at least one database the enrollment data; and

storing in the at least one database the enrollment data.

93.   (New) The method of claim 92, wherein the reference is a record of at least one of a government issued identification data, a driver's license data, a passport data, a birth certificate data, and a credit data.

94.   (New) The method of claim 92, wherein the enrollment data comprises at least one of a driver's license data, a social security number, an address, and a phone number.

95.   (New) The method of claim 92, wherein the enrollment data is acquired via a process selected from the group consisting of swiping, scanning and hand-keying.

96.   (New) The method of claim 92, wherein the system user additionally proffers an age presenter identification code.

97.   (New) The method of claim 96, wherein the age presenter identification code comprises at least one of a unique number and a reasonably unique number.

98.   (New) The method of claim 92, wherein the step of storing the enrollment data in the at least one database comprises:

converting the at least one biometric sample into a biometric template; and

saving the biometric template to the at least one database.

99.   (New) The method of claim 92, where in the enrollment data comprises a digital image of the at least one biometric sample.

100.   (New) The method of claim 92, wherein the enrollment data comprises a record maintenance password.